NORTH DAKOTA

HOMELAND SECURITY

ANTI-TERRORISM SUMMARY

The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

QUICK LINKS

North Dakota

Fire under control at metal galvanizing plant in West Fargo. A fire that heavily damaged a metal galvanizing plant in West Fargo, North Dakota, November 22 was under control, and hazardous materials inside were contained as of the morning of November 23. An estimated 60 firefighters and hazmat crew members spent the night battling the fire at K&K Galvanizers in West Fargo's industrial park. Officials were concerned about the plume of smoke from the fire because the building was reported to contain hydrochloric acid, sodium hydroxide, and zinc used in the galvanizing process. A CodeRED alert advised people downwind to take shelter. Crews also built dikes to contain some hydrochloric acid that was released, according to the city's assistant police chief. Source: http://www.westfargopioneer.com/event/article/id/19243/

Regional

(Minnesota) **Corn Plus admits faking pollution data.** Minnesota ethanol maker Corn Plus pleaded guilty November 23 to a federal felony charge of falsifying air pollution monitoring data and must pay $760,000 in fines and penalties. Corn Plus paid a $450,000 criminal fine levied by a federal judge, and has 30 days to pay a separate $310,000 civil penalty imposed by the Minnesota Pollution Control Agency, whose investigation helped uncover the violations. The farmer-owned cooperative, based in Winnebago, will remain on probation in the criminal case for 3 years. Two managers and a plant worker have been fired over the falsification, but have not been charged. Deliberate faking of monitoring records is extremely rare, state officials said. Under a plea bargain with the U.S. attorney's office, current Corn Plus employees and board members will not face prosecution. The deal leaves open the possibility of charges against fired employees, including the former general manager and former environmental compliance manger. In its plea, Corn Plus admitted its employees filed false reports in 2009 and 2010 indicating control equipment, known as bag houses, was working properly. A company spokesman said false monitoring logs also were created for the plant's scrubbers, which remove volatile organic compounds. The latest fines come on top of an $891,00 civil penalty and a $150,000 criminal fine for a 2009 federal misdemeanor conviction over Corn Plus' failure to prevent a wastewater discharge that had a high biological oxygen demand — a measure of its nutrient richness — into a drain that emptied into Rice Lake. Source: http://www.startribune.com/business/134398903.html?source=error

(Minnesota) **Xcel finds reason for shutdown of Monticello nuclear plant.** The Nuclear Regulatory Commission (NRC) said November 21 its on-site inspectors at the Monticello Nuclear Generating Plant in Monticello, Minnesota, were monitoring an unplanned shutdown of the plant over the weekend of November 19 and 20. The plant shut down automatically November 19 when safety systems detected low oil pressure in its turbines, according to Xcel Energy. Xcel officials said the outage is not expected to be lengthy but declined to specify how long. The NRC also is trying to locate a part missing from a device used to monitor the level of nuclear reaction inside the reactor, according to an NRC spokesperson. The monitor, which is highly radioactive, was taken out of service for replacement. It typically is stored in the spent fuel reactor pool for safekeeping until it can be shipped to a disposal site. There is no indication the missing part is

outside of the pool — it simply could not be found in its designated location, so workers will search the entire pool. Source: http://www.twincities.com/business/ci_19383739

National

(Vermont) **Heavy wet snow knocks out power to 12,000 customers in eastern Vermont.** About 12,000 Central Vermont Public Service (CVPS) customers in Vermont were without power November 23. Heavy wet snow began building up and bringing down trees, tree limbs, and lines primarily in Windham and Windsor counties around 4:30 a.m. A large transmission fault occurred at about 7 a.m., affecting more than 5,500 customers. Crews were working to sectionalize that problem, and restore power. The towns of Dummerston, Jamaica, Cavendish, Chester, and Hartford were hit hardest, and Woodstock Town and Village, among others were without power due to the transmission fault. Source: http://www.manchesterjournal.com/ci_19395301

International

Terrorist-funded Filipino hackers arrested. U.S. and Philippine authorities managed to arrest four members of a hacker collective suspected to have been funded by terrorists and to have attempted a hack on AT&T, Softpedia reported November 25. The investigation that led to the arrest of the Filipinos started in March when the FBI requested the aid of Criminal Investigation and Detection Group's Anti-Transnational and Cyber Crime Division (CIDG-ATCCD) concerning a hacking operation that targeted the wireless services provider AT&T. The suspects, aged between 21 and 31, and allegedly financed by a Saudi Arabian terrorist group, caused $2 million in damages, the Manila SunStar reported. The hackers were taken into custody after the FBI and the ATCCD raided several locations in the Metro Manila area, from where numerous computer and telecommunications equipments, believed to be used in the attacks, were seized. One of the hackers was arrested before in 2007 as a result of an operation by the FBI and Philippines authorities against terrorist organizations. The ATCCD chief claimed that back in 1999 when the FBI was investigating a series of hacking operations that targeted telecoms companies, they uncovered a trail of banking records that linked local hackers to terrorists. It turns out the criminal organizations from Pakistan and India are also somehow connected, since in 2007, a Pakistani man suspected of funding operations in India, also supplied the necessary funds for the Filipinos. Source: http://news.softpedia.com/news/Terrorist-Funded-Filipino-Hackers-Arrested-236560.shtml

Emergency condenser at Fukushima plant may not have fully run after tsunami. An emergency cooling condenser at the Fukushima No. 1 Nuclear Power Plant in Japan appears to have only partially run after the loss of all external power sources caused by the March 11 tsunami, the plant's operator said November 23. The two systems comprising the isolation condenser (IC) were found to have coolant levels of 65 and 85 percent when Tokyo Electric Power Company (TEPCO) employees examined the plant October 18. Noting that water has not been supplied to either of the systems since the disasters, TEPCO officials said they suspect the IC in the No. 1 reactor functioned only at a limited level over a short period. As to the cause of

the suspected malfunctioning, TEPCO suggested hydrogen generated by damaged nuclear fuel may have gathered in the piping, causing the IC's heat removal efficiency to decline. During the inspection, workers found no damage to the IC in the No. 1 reactor. Source: http://mdn.mainichi.jp/mdnnews/news/20111123p2a00m0na010000c.html

Banking and Finance Industry

'PayPal email address change' phishing scheme doing rounds. PayPal users have been targeted again as e-mails supposedly sent by the online payment company urge them to fill out a form with their personal and financial information to prevent the suspension of their accounts, Help Net Security reported November 25. With "You have changed your PayPal email address" in the subject line, the sender attempts to convince the recipient that someone has accessed their account and changed the e-mail address. To "keep the original email and restore their PayPal account," the users must fill out an attached Personal Profile Form - PayPal-.htm form. For everything to go smoothly, the sender also "helpfully" notes "the form needs to be opened in a modern browser which has javascript enabled (ex: Internet Explorer 7, Firefox 3, Safari 3, Opera 9)." But for those who fall for this scam, the submitted information gets sent directly to the phishers, Sophos points out. Source: http://www.net-security.org/secworld.php?id=12003

Ammonia-filled balloon used to rob Dallas Twp. bank. A man used a balloon he claimed was filled with "acid" as a threat to rob a Luzerne National Bank branch in Dallas Township, Pennsylvania, November 22. The suspect, who wore a two-tone black and dark gray jacket and concealed his identity with a black ski mask and a hood over his head, entered the bank and held up a balloon and told people in the bank it contained "acid," according to the Dallas Township police chief. After demanding cash, the balloon broke as the man left the bank, though it turned out to contain ammonia. The man escaped and was being sought by police November 23. Source: http://citizensvoice.com/news/ammonia-filled-balloon-used-to-rob-dallas-twp-bank-1.1236300#axzz1eXMmbFIF

Criminal probe into online mortgage scams widens. A criminal investigation into mortgage swindlers expanded beyond deceptive advertising on Google's Internet search engine to root out con artists who were luring their victims on Bing and Yahoo, the Associated Press reported November 21. News of the widening probe confirmed the Internet's three largest search engines were turned into tools of prey for crooks looking to bilk homeowners scrambling to avoid foreclosure. The scams involved online ads making bogus promises to help people hold onto their homes under a government-backed program to modify mortgage payments. After finding their victims using ads triggered by phrases such as "stop foreclosure," the swindlers extracted upfront fees or arranged to have the mortgage payments sent to them without providing any help. The crackdown shuttered 125 mortgage scams by November 21, up from 85 the week of November 14, when the Office of the Special Inspector General for the Troubled Asset Relief Program announced it was cleaning up misconduct on Google. The U.S. Treasury Department division said many con artists bought ads on all three search engines. Like Google, Microsoft's Bing search engine agreed to stop accepting ads from hundreds of Internet advertisers and agencies tied to the scams. The ban also applies to Yahoo, because it depends

on Microsoft to sell its search advertising as part of a revenue-sharing partnership. Source: http://www.google.com/hostednews/ap/article/ALeqM5jqtD1KZSDJ6Ccd5xJgDoxFmElrtQ?docId=726dd59cf33f4a318ecae159473800bf

Fake bank site spreads malware. On November 18, the Office of the Comptroller of the Currency (OCC) issued a warning about HelpWithMyBank.com, an illegitimate Web site feigning to offer consumer information about bank accounts and loans. Once visited, the HelpWithMyBank.com URL directs users to a legitimate consumer information site, HelpWithMyBank.gov, attempting to convince users they are connecting to a legitimate site, according to the OCC. But connecting to the fake site before the redirect is believed to expose consumers to malware. Source: http://www.bankinfosecurity.com/articles.php?art_id=4257

Chemical and Hazardous Materials Sector

(Connecticut) **Millstone investigates reactor restart failure.** Dominion, the owner of Millstone Power Station in Waterford, Connecticut, spent November 21 analyzing what went wrong November 20 that kept operators from restarting the Unit 3 reactor, which had been shut down for refueling. Operators halted the startup after an auxiliary steam boiler shut off unexpectedly, causing a loss of vacuum conditions used to run a condenser, according to a Dominion spokesman, and a spokesman for the Nuclear Regulatory Commission. The reactor had been shut down for several weeks, not only to replenish fuel in the reactor, but also to repair other equipment problems revealed during outage maintenance reviews. The company is continuing to isolate the cause of the problem while preparing to restart. Source: http://www.theday.com/article/20111122/BIZ02/311229919/1019&town=

Commercial Facilities

(California; South Carolina) **Shootings, pepper-spray attack mar Wal-Mart Black Friday sales.** As shoppers converged on retailers around the country looking for Black Friday deals November 24 and 25, authorities reported scattered problems. In Porter Ranch, California, a woman pepper sprayed customers at a Wal-Mart in what authorities said was a deliberate attempt to get more "door buster" merchandise. In San Leandro, California, a Wal-Mart shopper walking to his car was shot and wounded in a suspected robbery early November 25. Another shooting was reported at a parking lot next to a Wal-Mart in South Carolina, also a suspected robbery attempt. Officials told WMBF 32 Myrtle Beach, they believe the robbery was tied to Black Friday. At Porter Ranch, 20 customers, including children, were hurt in the 10:10 p.m. incident, officials said. Shoppers complained of minor skin and eye irritation, and sore throats. The woman used the spray in more than one area of the Wal-Mart "to gain preferred access to a variety of locations in the store," said a Los Angeles fire captain. Police were searching for the woman but said they have had trouble getting a clear description of her. Black Friday sales began at the Wal-Mart at 10 p.m. Source: http://latimesblogs.latimes.com/lanow/2011/11/wal-mart-black-friday-marred-by-shootings-pepper-spray-attack-.html

Communications Sector

AT&T says attempted hack of customer accounts failed. AT&T November 21 acknowledged an organized attempt to hack information on fewer than 1 percent of its 100 million wireless customers, but it said no accounts were breached. A spokesman said the hackers appear to have used auto-script technology to find whether AT&T telephone numbers were linked to online AT&T accounts. He did not elaborate, but said an investigation is continuing. The spokesman said fewer than 1 percent of AT&T's 100.7 million wireless subscribers were contacted by hackers through e-mail — a number that could mean about 1 million customers were affected. "Our investigation is ongoing to determine the source or intent of the attempt to gather this information," the AT&T spokesman said. He said the AT&T account holders were advised of the attempt "out of an abundance of caution." Source: http://www.computerworld.com/s/article/9222079/Update_AT_T_says_attempted_hack_of_customer_accounts_failed

Critical Manufacturing

Motion sensing wall switches recalled by HeathCo due to electrical shock hazard. The U.S. Consumer Product Safety Commission, in cooperation with HeathCo, November 22 announced a voluntary recall of about 75,000 Heath/Zenith and Wireless Command motion sensing wall switches. Consumers should stop using recalled products immediately unless otherwise instructed. When the switches are in the auto mode and the light is off, a small amount of leakage current passes through the electric circuit, including the socket. If consumers fail to disconnect the power at the circuit breaker and make contact with both terminals inside the socket while replacing the bulbs, there is a risk of an electric shock. Consumers should stop using the recalled wall switches
and contact HeathCo for a free replacement. Source: http://www.cpsc.gov/cpscpub/prerel/prhtml12/12046.html

Defense/ Industry Base Sector

Nothing Significant to Report

Emergency Services

(California) **Hacker group Anonymous targets UC-Davis pepper-spray cop.** The rogue hacker group known as Anonymous posted a YouTube video disclosing the cellphone number, e-mail, and home address of the University of California (UC), Davis police officer who sparked worldwide outrage when he pepper-sprayed a group of student protesters over the weekend. The video, which was posted November 22, has since been removed because it is "a violation of YouTube's policy prohibiting hate speech." Anonymous has threatened or claimed credit for attacks on numerous media organizations, including Fox News — but this appears to be the first time the hacking group has targeted an individual. "Expect our full wrath," the video states. "Anonymous seeks to avenge all protesters. We are going to make you squeal like a pig." The

lieutenant and another officer were placed on administrative leave following the weekend clash with protesters on the UC-Davis campus. Source: http://news.yahoo.com/blogs/cutline/anonymous-hackers-target-uc-davis-pepper-spray-cop-181722285.html

(California) **Another prison riot at Pelican Bay.** Dozens of inmates rioted at Pelican Bay, California, State Prison November 22, the second uprising in 9 days. The brawl involving an estimated 50-75 inmates around 7 a.m. in the minimum support facility, a dormitory setting area housing non-violent offenders, said the prison's public information officer. Force was not needed to stop the inmates, he said. "Officers responded ... and when they responded all the inmates got down on the ground and stopped fighting with each other," The riot lasted about 5 minutes, he added. Four inmates were injured; one was admitted to Sutter Coast Hospital for a higher level of care, and the rest were treated at the prison's medical facility, he said. This riot had no connection with the November 20 riot, when 63 inmates attacked each other on the general population yard A, which houses maximum-security inmates, he said. The prison's investigative services unit and the Del Norte County District Attorney's Office are investigating. Source: http://www.triplicate.com/News/Breaking-News/Another-prison-riot-at-Pelican-Bay

ENERGY

EPA accepts environmental petition on fracking chemicals. The Environmental Protection Agency (EPA) said it will weigh rules requiring disclosure of the chemicals used in hydraulic-fracturing fluids. Companies such as Halliburton Co. and Schlumberger Ltd., which supply oil and natural-gas producers, should be required to reveal substances used in the mining technology known as fracking, according to a petition filed with the EPA by the environmental group Earthjustice. In a response posted on its Web site November 23, the EPA said it will begin gathering that data. The EPA will try to provide "aggregate pictures of the chemical substances and mixtures used in hydraulic fracturing," an assistant administrator said. The EPA turned down another part of the organizations' request, telling the groups on November 2 it would not mandate toxicity testing for each of the chemicals. Extraction from shale formations has grown to about 15 percent of U.S. natural-gas production and this share is expected to triple by 2035, according to the U.S. Energy Information Administration. Source: http://www.businessweek.com/news/2011-11-24/epa-accepts-environmental-petition-on-fracking-chemicals.html

(Louisiana) **Vandals target Beauregard oil well, cause spill.** Beauregard Parish, Louisiana sheriff's officials responded November 20 to a vandalism call from an oil-well site off Highway 389 near DeQuincy. The caller said someone vandalized the oil site, creating a major spill. Sources said 220 barrels were spilled. Environmental issues are not expected since sites like these are normally encircled by a berm. Hazmat teams were called out to clean up the mess. Source: http://www.wafb.com/story/16094506/vandals-target-beauregard-oil-well-cause-spill

EPA proposes operator training, stronger containment regulations for storage tanks. The Environmental Protection Agency (EPA) is proposing to strengthen regulations governing

underground storage tanks (USTs), adding new rules for backup containment and extending training requirements to more storage tank owners and operators. State agencies that accept federal grant money are required under current regulations to set operator training requirements under the Energy Policy Act, but the requirements do not cover underground tanks on tribal lands and in states that do not accept federal funds. The proposed revisions would implement training requirements nationwide. The proposed regulations would apply to tanks that hold petroleum or hazardous chemicals, which are regulated under Subtitle I of the Resource Conservation and Recovery Act (RCRA). They would not affect USTs containing hazardous waste, which are regulated under RCRA Subtitle C. The EPA published the proposed rule November 18. It expects to issue a final rule in 2013. There are about 595,000 active USTs at an estimated 214,000 sites in the United States, according to the EPA. The agency estimates the compliance costs of the proposed rule would amount to $210 million annually, but said the proposal would lead to $300 million to $770 million in avoided remediation costs. Motor fuel retailers, which account for about 80 percent of UST systems, are expected to bear a majority of the cost. Source: http://www.bna.com/epa-proposes-operator-n12884904444/

Food and Agriculture

(New York) **Chicken products recalled for misbranding.** Berk Lombardo of Brooklyn, New York is recalling about 1,080 pounds of uncooked stuffed chicken breasts because of misbranding and undeclared ingredients, including known allergens. The chicken products may contain eggs, milk, monosodium glutamate (MSG), or soy, which are not noted on the label. MSG is not classified as an allergen, but can cause a brief reaction in people with a sensitivity to it. The U.S. Department of Agriculture's (USDA) Food Safety and Inspection Service (FSIS) discovered the problem during a label review at the company. The FSIS and the company have received no reports of adverse reactions due to consumption of these products. The recalled products, which were sold directly to individual households throughout Long Island, include: Boxes containing four, 6-oz. frozen, vacuum-sealed packages of "CHICKEN BREAST STUFFED BROCCOLI & CHEESE" that bears the establishment number "P-19034" inside the USDA mark of inspection; boxes containing four, 6-oz. frozen, vacuum-sealed packages of "CHICKEN BREAST with rib meat CORDON BLEU BREADED" that bears the establishment number "P-19034" inside the USDA mark of inspection; and boxes containing four, 6-oz. frozen, vacuum-sealed packages of "STUFFED CHICKEN BREAST KIEV" that bears the establishment number "P-19034" inside the USDA mark of inspection. Source: http://www.foodsafetynews.com/2011/11/chicken-products-recalled-for-misbranding/

(New York) **Allergen alert: Undeclared dairy in pineapple pastry.** Rio Grande Imports of Copiague, New York is recalling 50 cases of Semita de Pina because the pastries may contain undeclared dairy, Food Safety News reported November 23. The problem was discovered during routine sampling by New York State Department of Agriculture and Markets food inspectors. Subsequent analysis revealed the presence of the allergen in product packages that did not declare it on the label. Semita de Pina is a pineapple-filled pastry with the brand name El Triunfo packaged in a poly plastic boat with a clear plastic overwrap and a code of 11-22-11. It was distributed to the lower Hudson Valley Region, New York City boroughs, and Long Island.

Source: http://www.foodsafetynews.com/2011/11/allergen-alert-undeclared-dairy-in-pineapple-pastry/

179 Salmonella chicken liver cases in 6 states. Chicken livers contaminated with Salmonella Heidelberg have now sickened 179 people in 6 states, the Centers for Disease Control and Prevention (CDC) reported November 22. That is 22 more cases in 4 more states than the CDC reported November 9. The kosher broiled chicken livers, sold by Schreiber Processing Corp. of Maspeth, New York, under the MealMart brand, were recalled November 8. The chicken livers were distributed to New York, New Jersey, Pennsylvania, Maryland, Minnesota, Ohio, Rhode Island, and Florida. In its latest report on the outbreak, the CDC said New York now identified 99 cases of Salmonella infection linked to the chicken livers, New Jersey confirmed 61 related cases, Pennsylvania 10, Maryland 6, Ohio 2, and Minnesota 1. The illnesses began in March and continued through October. Source: http://www.foodsafetynews.com/2011/11/cdc-179-salmonella-chicken-liver-cases-in-6-states/

(Georgia) **Allergen alert: GFS sugar, coffee creamer mix up.** Diamond Crystal Brands of Savannah, Georgia, issued an allergen alert because of undeclared milk in 12-ounce GFS sugar canisters that were filled in error with non-dairy coffee creamer, Food Safety News reported November 22. Non-dairy coffee creamer contains sodium caseinate, which is a milk derivative. The items, which were shipped in 24-can cases include: case label: GFS Non-Dairy Coffee Creamer - 24/12 ounce - Lot G293 B located on the side of the case and canister label: GFS Sugar - Lot G293 B located on the bottom of the canister. Source: http://www.foodsafetynews.com/2011/11/allergen-alert-gfs-coffee-creamer-sugar-mix-up/

Government Sector (including Schools and Universities)

(Oklahoma) **Bomb squad called to Logan County Courthouse.** A bomb squad was called to the Logan County Courthouse in Guthrie, Oklahoma, November 23 after a pair of threatening phone calls was made, a fire official said. The Guthrie fire chief said the scene was cleared by about 4:15 p.m., and that the bomb squad was asked to search the courthouse after a pair of threatening phone calls had been received. He said the two calls came in at 1:50 and 2:18 p.m. and that the caller's voice was computer-generated. The caller told the court clerk, "Allah is God. Allah is alive. Everyone will burn." The FBI has been asked to help investigate. Source: http://www.koco.com/mostpopular/29846616/detail.html

Obama security booklet discovered in gutter in Australia's capital. The Australian government launched an investigation November 20 into how a classified booklet detailing the U.S. President's itinerary came to be lost in a gutter during the president's visit to Canberra, Australia, the week of November 14. A journalist with the Age newspaper reported he found the 125-page booklet November 17 about 100 yards from Parliament House in Canberra, where the President attended several functions during his 27-hour Australian visit. The booklet contained details on his itinerary, his security convoy, and the cell phone numbers of senior U.S.

and Australian officials. An analyst based at Sydney University, described the incident as a "significant security breach." Australia's attorney-general's department said in a statement November 20 it was investigating. Source: http://www.msnbc.msn.com/id/45374668/ns/politics-white_house/#.Ts0ElVZinus

(Maine) **Teenage girl charged with arson.** Maine fire investigators charged a 13-year-old girl with arson for allegedly setting fire to toilet paper at her school, forcing the entire school to be evacuated. Officials with the state fire marshal's office said the fire started in a toilet-paper dispenser in a second-floor girl's bathroom at Vassalboro Community School in Vassalboro More than 500 students were evacuated. The fire was confined to the bathroom. No injuries were reported. Officials said the seventh-grade girl will appear in juvenile court in February. Source: http://www.wgme.com/news/top-stories/stories/wgme_vid_10044.shtml

(South Carolina) **Suspicious package shuts SC school for 2nd day.** A suspicious package has led officials to cancel classes at a Columbia high school for the second time in less than a month in Columbia, South Carolina. The package was found November 21 before classes started at Eau Claire High School. Police closed a road in front of the school as they investigated. Richland School District 1 originally announced a 2-hour delay, but decided to cancel classes about 2 hours later. Eau Claire students also missed a day October 31 after a suspicious package was found. Police detonated the package, but never said what was inside. Source: http://www.wftv.com/ap/ap/education/suspicious-package-shuts-sc-school-for-2nd-day/nFjNt/

(Colorado) **Colo. barricaded airman suspect is awaiting sentencing on attempted sex exploitation of child.** The U.S. Air Force said it is investigating how an airman managed to get his own handgun onto a sensitive air base in Colorado where he barricaded himself in a building for 10 hours before surrendering. The airman was taken into custody at Schriever Air Force Base near Colorado Springs, Colorado, at about 8 p.m. November 21, officials said. No injuries were reported. The base, about 60 miles south of Denver, controls more than 60 military satellites, including those used for GPS. The Air Force said satellite operations were not disrupted. Officials said the suspect was in a building where personnel prepare for deployment. The satellite control rooms are in a separate, heavily guarded area. Authorities said the airman faces a possible discharge for an unrelated crime in civilian court. He is being held in the Teller County jail in Divide, Colorado, under an agreement between the county and the Air Force base. Air Force officials did not say whether the suspect will face prosecution in civilian or military court over the standoff. Personal weapons are forbidden on the base. The suspect is a member of the 50th Security Forces Squadron, and has been in the Air Force for 2 years and 9 months, officials said. Source: http://www.washingtonpost.com/national/after-standoff-air-force-investigates-how-airman-got-handgun-onto-sensitive-colorado-air-base/2011/11/22/gIQAQfk3kN_story.html?tid=pm_national_pop

INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

Thanksgiving menaced by virus-laden fake iTunes vouchers. E-mails containing supposed iTunes gift certificates doing the rounds in the run-up to Thanksgiving were actually loaded with

malware, The Register reported November 24. Spoofed e-mails purportedly offering $50 vouchers for the iTunes Store, which arrive with e-mail subject lines such as “iTunes Gift Certificate,” come with an attachment supposedly containing a certificate code. In reality, these zip file attachments are infected with the Windows PC-compatible malware, detected by Sophos as BredoZp-B and first spotted by German info security group eleven-security. Source: http://www.theregister.co.uk/2011/11/24/fake_itunes_gift_cert_malware/

Android monitoring software hides SMS trojan. Kaspersky Lab experts came across a legitimate application used for monitoring and managing SMSs, calls and Internet traffic on an Android smartphone that can masquerade a malicious Trojan once it lands on a device. The Trojan sends messages to premium rate numbers. The application targets users from countries such as Belgium, France, Switzerland, Luxemburg, Germany, Spain, and Canada, which means the cybercriminals moved their operations from China and Russia to Europe and North America. Upon closer inspection, the app hosted on the Web as SuiConFo, was hiding a SMS trojan identified as Trojan-SMS.AndroidOS.Foncy, which sends four short messages to premium rate numbers. To make the software as legitimate looking as possible, its creators made sure an icon appears in the phone’s menu, but once it is launched, an error pops up, claiming the Android version is not compatible. Right after the error, the trojan will use two public methods to determine the ISO country code of the SIM card. Based on this code, it will send the four MSs to one of eight locations. The malware will not only send short messages, but it will also hide incoming SMSs from certain numbers. This is done to ensure reply messages received from premium numbers are not seen by the victim. The virus is programmed to send alerts to a French cell phone number, based on the replies sent by the premium numbers so the developers are aware of the number of victims. Because such trojans can generate a considerable income, it is likely these operations will be extended to affect citizens of other countries. Source: http://news.softpedia.com/news/Android-Monitoring-Software-Hides-SMS-Trojan-236641.shtml

Google protects HTTPS-enabled services against future attacks. Google modified the encryption method used by its HTTPS-enabled services including Gmail, Docs, and Google+ in order to prevent current traffic from being decrypted in the future when technological advances make it possible, IDG News Service reported November 23. The majority of today's HTTPS implementations use a private key known only by the domain owner to generate session keys that are subsequently used to encrypt traffic between the servers and their clients. This approach exposes the connections to so-called retrospective decryption attacks. "In 10 years time, when computers are much faster, an adversary could break the server private key and retrospectively decrypt today's email traffic," explained a member of Google's security team. To mitigate this relatively low, but real security risk, Google implemented an encryption property known as forward secrecy, which involves using different private keys to encrypt sessions and deleting them after a period of time. In this way, an attacker who manages to break or steal a single key will be unable to recover a significant quantity of e-mail traffic that spans months of activity, the member of Google's security team said. Source: http://www.computerworld.com/s/article/9222129/Google_protects_HTTPS_enabled_services_against_future_attacks

FFmpeg updates fix security bugs. Versions 0.7.8 and 0.8.7 of the open source FFmpeg tool and library collection have been released. According to a news post on the project's homepage, the maintenance and security updates to the 0.7.x and 0.8.x branches of FFmpeg fix a number of bugs found in previous releases and address three vulnerabilities. The updates correct issues that could be exploited by an attacker to cause a denial-of-service condition or potentially compromise an application that uses FFmpeg –- well-known open source software that uses the library collection and includes the VLC Media Player, MPlayer, and Perian. An attack on FFmpeg would typically require the user to open a maliciously crafted media file or streaming URL. The vulnerabilities addressed in the update include errors in the QDM2 decoder and "vp3_dequant()" function that could be used to trigger a buffer overflow, as well as a problem in a number of functions that could lead to out-of-bounds reads. Source: http://www.h-online.com/security/news/item/FFmpeg-updates-fix-security-bugs-1382715.html

Xbox Live accounts targeted by massive phishing campaign. There is much confusion related to the issue of Xbox live accounts forcefully taken by cybercriminals, Softpedia reported November 23. While some feared a massive hacking operation was behind the incident, Microsoft claims the accounts fell victim to phishing. Xbox forums have been flooded with complaints from members who believe their accounts were taken over by hackers, but the official Xbox Live UK Facebook page claims no hacking was involved. The Sun published an article in which they revealed many users around the world reported the credit cards attached to their Live accounts were used to make small purchases, the average loss being estimated at $80 per account holder. In response to the article, Xbox UK issued a statement denying Xbox Live was hacked. “Microsoft can confirm that there has been no breach to the security of our Xbox LIVE service. In this case, a number of Xbox LIVE members appear to have recently been victim of malicious ‘phishing’ scams,” reads the statement. Source: http://news.softpedia.com/news/Xbox-Live-Accounts-Targeted-By-Massive-Phishing-Campaign-236130.shtml

Android’s a malware magnet, says McAfee. Malware targeting Android devices continues to surge, according to a new report from McAfee, pushing 2011 to become the busiest year in history for mobile and general malware. The amount of malware infecting Android devices during the third quarter grew almost 37 percent from the second quarter, according to McAfee’s Third-Quarter Threats Report. Android’s growing demand among consumers has made it an increasingly ripe and inviting target for cybercriminals — almost all new mobile malware over the third quarter was aimed squarely at Android. Among all mobile platforms, Nokia’s Symbian OS still saw the greatest amount of malware. As a result of the onslaught against Android and the growth in overall malware, McAfee believes the industry will see 75 million unique pieces of malware by the end of the year, up from its previous forecast of 70 million. Phony antivirus products, AutoRun malware, and password-stealing trojans were among the most common types of malware in the quarter, staging a rebound from previous quarters. Malware aimed at the Mac also continues to grow. The number of botnet infections inched down over the third quarter but staged dramatic gains in countries such as Argentina, Indonesia, Russia, and Venezuela. Cutwail, Festi, and Lethic proved to be the most dangerous

and damaging botnets last quarter. Though spam dropped in numbers since 2007, it has grown in sophistication, according to McAfee. Spearphishing, or targeted spam, is increasingly being adopted by more attackers and is proving to be highly effective. Source: http://news.cnet.com/8301-1009_3-57328575-83/androids-a-malware-magnet-says-mcafee/

National Monuments and Icons

(Arizona) **GAO report links Arizona wildfires to immigrants.** A study by Congress' investigative arm shows investigators have linked 30 fires that erupted in a 5-year period in Arizona's border region to people who crossed into the United States illegally, the Associated Press reported November 22. The U.S. Government Accountability Office (GAO) gathered information for the study, which included fires within 100 miles of Arizona's border with Mexico, from the National Interagency Fire Center in Boise, Idaho, and interviewed federal, state and tribal officials along the state's 370-mile border. Nearly 2,500 wildfires occurred in the Arizona border region from 2006 to 2010, but the GAO studied only those that were human-caused, burned more than an acre, and those for which investigative reports were available. Of the 422 wildfires that topped an acre, federal investigators probed 77, or 18 percent. The GAO found that 30 of the probed wildfires were linked to illegal border crossers primarily in southeastern Arizona based on what was written in investigative reports. Fifteen were thought to be a signal for help, provide warmth, or cook food. An investigative report on the 2009 Bear fire backed up that suspicion by noting the discovery of discarded bottles and food wrappers with Spanish language labels near a campfire. It also noted the area is frequented by illegal border crossers, and is adjacent to a heavily used smuggling trail, the GAO report said. Reports on the other 15 wildfires do not give a reason for the start of the fire, but the GAO said a couple of them mention that the areas of ignition are known for drug smuggling. Source: http://abcnews.go.com/US/wireStory/ap-exclusive-report-links-wildfires-immigrants-15005836#.Tsz-lFZhIW9

Postal and Shipping

Nothing Significant to Report

Public Health

Merck will pay $950M to settle Vioxx investigation. The Department of Justice (DOJ) said November 22 that drugmaker Merck will pay $950 million to resolve investigations into its marketing of the painkiller Vioxx. The agency said Merck will pay $321.6 million in criminal fines, and $628.4 million as a civil settlement agreement. It will also plead guilty to a misdemeanor charge it marketed Vioxx as a treatment for rheumatoid arthritis before getting approval from the U.S. Food and Drug Administration. The government will get $426.4 million from the settlement, and $202 million will be distributed to state Medicaid programs for 43 states, and the District of Columbia. Merck stopped selling Vioxx in September 2004 after evidence showed the drug doubled the risk of heart attack and stroke. In 2007, the company paid $4.85 billion to settle around 50,000 Vioxx-related lawsuits. The DOJ said the settlement resolves allegations that Merck made false, unproven, or misleading statements about Vioxx's

safety to increase sales, and made false statements to Medicaid agencies about its safety. Source: http://www.businessweek.com/ap/financialnews/D9R60O8O0.htm

Transportation

FAA limits emergency oxygen on planes. Airlines earlier this year quietly removed the emergency oxygen from lavatories because of concerns it could be used to start a fire, USA Today reported November 24. Safety officials now are working with aircraft manufacturers to develop a secure oxygen system. It will take 2-4 years to complete the job, the Federal Aviation Administration (FAA) says. That is not fast enough for safety advocates and flight attendants. They are concerned someone using a lavatory could be seriously harmed or killed if there is an aircraft decompression and emergency oxygen is needed immediately. The FAA ordered airlines to remove the chemical oxygen generators in lavatories because they "were easily accessible and could have been manipulated to create a flight hazard." The decision, made in conjunction with the Transportation Security Administration (TSA) and the FBI, "was purely a precautionary measure," and "there is no credible or specific threat at this time," the FAA said in written responses to USA Today questions. The agency "expects that it will take between two and four years to design, develop and install a secure lavatory oxygen system in all U.S. operated passenger aircraft," it said. Removal of oxygen from lavatories, each of which was equipped with two oxygen masks, did not affect oxygen stored above passenger seats. Source: http://tucsoncitizen.com/usa-today-news/2011/11/24/faa-limits-emergency-oxygen-on-planes/

Water and Dams

(Texas) **Was the three character password used to hack South Houston's water treatment plant a Siemens default?** Siemens said November 22 it is working with the DHS to investigate a cyber intrusion into a water treatment plant in South Houston, Texas, but could not confirm a default, three-digit password, hard coded into an application used to control the company's supervisory control and data acquisition (SCADA) software played a role. The hacker, who goes by the handle "pr0f," described using an easy-to-crack three-character password that provided access to Siemens Simatic HMI (human machine interface) software. That description matches that of the default password assigned to new user accounts with Sm@rtService and Sm@rtClient, two applications used to remotely access Simatic HMI WinCC installations, according to Siemens documentation reviewed by Threatpost. In a statement November 22, Siemens said it "is aware of" the breach in South Houston in which "control graphics screen shots were taken from the system and posted on the Internet." The company said it didn't know of any malicious actions associated with the breach, but that it is in "close contact" with the U.S. Industrial Control Systems Cyber Emergency Response Team to support "ongoing investigations about the incident," Siemens said. A Siemens spokesman could not confirm the hack took advantage of a default password used by the application, or one configured by officials in South Houston. However, he acknowledged that older versions of the WinCC application use three-character default passwords. Source:

http://threatpost.com/en_us/blogs/was-three-character-password-used-hack-south-houstons-water-treatment-plant-siemens-default-11

(Wisconsin; Michigan) **Debris on Michigan beaches tied to Milwaukee sewer overflows.** Some of the debris that washed up on Michigan beaches in 2008 and 2010 likely came from Milwaukee sewer overflows, federal investigators concluded in documents released November 21 by the Chicago-based Alliance for the Great Lakes. According to the Milwaukee Journal Sentinel, a 2011 U.S. Coast Guard summary of the investigations identifies combined sewer overflows in June 2008 and July 2010 as a "logical suspect" in releasing debris to the lake that later washed ashore in Michigan, the Alliance said in a statement on its Web site. A National Oceanic and Atmospheric Administration analysis of lake tides, currents, and winds after both overflows concluded the debris might have come from Milwaukee at around the time of the overflows, according to investigation documents. An estimated 2.9 billion gallons of untreated sewage and storm water flowed to the lake over 9 days — June 7 to 15 — in the largest combined sanitary and storm sewer overflow since the deep tunnel system opened in 1994. The district's separate sanitary sewers released 686 million gallons of untreated sewage and storm water to the lake during overflows from June 7 to 9, 2008. Torrential rains were blamed in a July 22 to 25, 2010, combined sewer overflow of 1.985 billion gallons, and a separate sewer overflow of 171 million gallons. The Alliance acknowledged that Milwaukee Metropolitan Sewage District's (MMSD) state permit allows up to six combined sewer overflows in a year. Source: http://www.jsonline.com/news/milwaukee/debris-on-michigan-beaches-tied-to-milwaukee-sewer-overflows-nh35971-134289978.html

(Texas) **Central Texas town may run out of water.** The record-setting drought that has overtaken the entire state of Texas has left 11 communities on a state agency list of cities at risk of running out of tap water in 6 months, the Houston Business Journal reported November 21. According to the Texas Commission on Environmental Quality, Groesbeck and its population of 6,000 residents, is on schedule to tap out December 6, if there is no significant rainfall. The state's worst 1-year drought on record has almost dried up Fort Parker Lake, which is fed by the Navasota River that normally flows into catchment that serves the lake. At the beginning of the summer, Fort Parker Lake was filled to capacity. Source: http://www.bizjournals.com/houston/morning_call/2011/11/central-texas-town-may-run-out-of-water.html

North Dakota Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: North Dakota State and Local Intelligence Center: 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov; Fax: 701-328-8175 State Radio: 800-472-2121; Bureau of Criminal Investigation (BCI): 701-328-5500; North Dakota Highway Patrol: 701-328-2455; US Attorney's Office Intel Analyst: 701-297-7400; Bismarck FBI: 701-223-4875; Fargo FBI: 701-232-7241.

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, 701-328-8168